UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,837	08/18/2006	Frederic Beun	MM6019PCT	2806

79681 7590 08/18/2011

David A. Einhorn, Esq.
Baker & Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
08/18/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

deinhorn@bakerlaw.com
Patents-BakerHostetler@bakerlaw.com
IPGNYG@bakerlaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/589,837	BEUN ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 June 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1,5-8,10-18 and 24-47* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,5-8,10-18 and 24-47* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/589,837 is presented for examination by the examiner. Claims 36 and 39 have been amended. Claims 1, 5-8, 10-18, and 24-47 are pending.

Response to Amendment

Claim Objections

Claims 40 and 41 are objected because they now do not properly refer back to amended claim 39. As such the computer program lacks antecedent basis.

Response to Arguments

Applicant's arguments filed 6/2/11 have been fully considered but they are not persuasive. It is noted that in the arguments claim 42 is said to be dependent from claim 39. However, claim 42 is an independent claim and has not been amended as the other independent claims. As such, with no arguments specified for claim 42 that rejection is maintained.

With respect to the independent claim 1and 36, the Applicant alleges Tsuria and Kahn fail to teach the idea of pairing a plurality of external security modules to a

decoder. Applicant argues the combination of Kahn and Tsuria is faulty. Kahn receives a lists of authorized security modules into the data reception equipment. As later generations, selective lists are used to identity CAMs which can be paired to an IRD while preventing others from being paired because of their security demise (0043). Khan matches the unique identifier of a CAM to the list, so in fact the list is actually how pairing is controlled. CAMs must have a unique identifier to allow them to be selectively removed from the authorized list. The presented arguments, take the position that the pairing of multiple security modules occurs in a concurrently. That is to say, two or more security modules can actively be paired and used with one reception equipment. However the claim language is still so broad that it reads on the well accepted teachings of Kahn which speaks to the natural progression of new security modules replacing older generations. If it is intended for the instant invention to pair multiple security modules to a single reception equipment, and have each actively paired wherein each of the modules can be swapped out for another modules and the IRD maintains its pairing throughout, this feature needs to be amended into the claim language. The act of just pairing multiple security modules still reads on pairing one security module to a reception equipment and then at some later time another security module is paired to the reception equipment. This is well established in the art and different from having a data equipment simultaneously paired and able to operate with to more than one security module at any given time.

With respect to amended claims 29 and 39, the above arguments apply as well. It is now being rejected in view of Tsuria and now Kahn.

With respect to claim 33, the claim language still reads on Tsuria and his teaching of activating using chaining data two security modules at a single reception equipment (col. 7, lines 45-58).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 5-8, 10-18, and 24-32, 36-41, and 43-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 6,405,369 to Tsuria in view of USP Application Publication 2006/0161976 to Kahn et al., hereinafter Kahn.

As per claim 1, Tsuria teaches a method for an operator to dynamically and remotely control the pairing of digital data reception equipment (2) with one or more external security modules (6, 8) each having a unique identifier (col. 3, lines 3-15) and with each security module being adapted to cooperate with said digital data reception equipment for controlling reception of distributed data by means of said digital data

reception equipment and with the digital data reception equipment having a computer and stored program [decoder and programmed for activation; col. 7, lines 35-38], method comprising the following steps (col. 1, lines 54-65):

using the computer to verify whether or not the identifier of said external security modules is memorized in the digital data reception equipment upon connection of said external security modules to the digital data reception equipment [second card is inserted in to the receiver to validate and identify the signature of said second card; col. 7, lines 44-53],

if the unique identifier of the external security modules is memorized in the digital data reception equipment, transmitting a control signal to the digital data reception equipment defining configuration parameters to activate the pairing of the said digital data reception equipment with said external security modules [chaining data; col. 7, lines 45-48];

if the unique identifier of the external security modules is not memorized in the digital data reception equipment, transmitting a control signal to the digital data reception equipment defining configuration parameters to deactivate the pairing of the said digital data reception equipment with said external security modules [inherent that if the smart card's signature is not validated, there will be no pairing; col. 5, lines 15-18 and col. 7, lines 45-48]; wherein

said configuration parameters include at least one of the following set values: - authorize memorization, - prohibit memorization, - erase identifiers previously memorized in the reception equipment (2), - activate or deactivating the check phase

(col. 3, lines 27-31) including a procedure consisting of disturbing the data processing if the identifier of the connected external security module (6, 8) is not previously memorized in the reception equipment (col. 5, lines 10-15).

With respect to the claim, Tsuria fails to teach pairing more than one security module to a particular reception equipment and transmitting an updated list of external security module identifiers to the digital data reception equipment. Kahn teaches pairing more than CAM (security module) to an IRD (digital reception equipment) based on the generation of a selective list (0041). As an option, a selective list, converse to blacklists, can specify which CAMs an IRD can successfully pair with. As later generations, selective lists are used to identity CAMs which can be paired to an IRD while preventing others from being paired because of their security demise (0043). Kahn shows that and IRD can contain a list of all the CAMs that it may pair with. Absent of being on the list, precludes a particular CAM from being paired. Kahn teaches that security modules that have been comprised/hacked/cloned can be removed from the selective list, effectively blacklisting them to prevent illegal content decoding. As such, it is advantageous to prevent security modules that have been compromised from successfully decoding protected content. Kahn teaches a way of doing this by using selective list identifying legitimate external security module identifiers. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results.

As per claim 5, Tsuria teaches that said signal also includes the maximum allowable number of memorized identifiers (col. 9, lines 5-8).

As per claim 6, Tsuria teaches signal includes a reconfiguration set value through which an updated list of identifiers of external security modules (6, 8) matched with the reception equipment(2) is transmitted to said reception equipment (col. 7, lines 29-35).

As per claim 7, Tsuria teaches list is transmitted directly to the reception equipment (col. 6, lines 55-59).

As per claim 8, Tsuria teaches list is transmitted through an external security module (6, 8) connected to said reception equipment (col. 6, lines 40-45).

As per claim 10, Tsuria teaches data are distributed without encryption or scrambled by an encrypted control word and in that each external security module (6, 8) includes access rights to said data and a decryption algorithm for said control word (col. 5, line s35-40).

As per claim 11, Tsuria teaches said signal is transmitted to a reception equipment (2) in an EMM message specific to an 25 external security module (6, 8) associated with this reception equipment (col. 6, lines 55-60).

As per claim 12, Tsuria teaches a signal is transmitted to a reception equipment (2) in an EMM message specific to this reception equipment (col. 6, lines 55-60).

As per claim 13, Tsuria teaches a given reception equipment (2) said list is transmitted in an EMM message specific to a security module (6, 8) associated with this reception equipment (col. 6, lines 55-60).

As per claim 14, Tsuria teaches a signal is transmitted to a group of reception equipment (2) in an EMM message specific to a group of external security modules (6, 8) associated with said reception equipment (col. 6, lines 55-60).

As per claim 15, Tsuria teaches signal is transmitted to a group of reception equipment (2) in an EMM message specific to said group of reception equipment (col. 6, lines 55-60).

As per claim 16, Tsuria teaches a given group of reception equipment (2), said list is transmitted in an EMM message specific to a group of external security modules (6, 8) associated with said reception equipment (col. 6, lines 55-60).

As per claim 17, Tsuria teaches said check signal is transmitted in a private flow processed by a dedicated software executable in each reception equipment as a function of the identifier of the external security module associated with said reception equipment (col. 6, lines 55-60).

As per claim 18, Tsuria teaches a given group of reception equipment (2), said list is transmitted in a private flow to each reception equipment (col. 6, lines 55-60).

As per claim 24, Tsuria teaches identifiers of external security modules (6, 8) are grouped in an encrypted list (col.2, lines 29-30).

As per claim 25, Tsuria teaches reception equipment (2) includes a decoder and the external security module (6, 8) includes an access control card (6) in which information about access rights of a subscriber to digital data distributed by an operator

is memorized, and in that matching is done between said decoder and said card (6). (col. 2, lines 46-50).

As per claim 26, Tsuria teaches that the reception equipment (2) includes a decoder and the external security module (6, 8) includes a removable security interface (8) provided with a non-volatile memory that can cooperate firstly with the decoder, and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator, and in that matching is done between said decoder and said removable security interface (col. 1, lines 55-60 and col. 2, lines 45-55).

As per claim 27, Tsuria teaches the reception equipment (2) includes a decoder provided with a removable security interface (8) with a non-volatile memory that can cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), and in that matching is done between said removable security interface (8) and said access control cards (col. 2, lines 45-55).

As per claim 28, Tsuria teaches the data are audiovisual programs (col. 1, line 50).

As per claim 29, Tsuria teaches a digital data reception equipment for pairing to one or more external security modules (6, 8) each having an unique identifier [signature] to manage access to digital data distributed by an operator (col. 1, lines 61-65 and col. 3, lines 1-5), comprising means for executing a computer program in a readable medium for:

verifying whether or not the identifier in said external security modules (6, 8) is already memorized in the digital data reception equipment (2) upon connection of said external security modules (6, 8) to the digital data reception equipment [second card is inserted in to the receiver to validate and identify the signature of said second card; col. 7, lines 44-53] ,

activating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier of the external security modules (6, 8) is already memorized in the digital data reception equipment (2) [chaining data; col. 7, lines 45-48] and

deactivating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier in the external security modules (6, 8) is not already memorized in the digital data reception equipment (2) [inherent that if the smart card's signature is not validated, there will be no pairing; col. 7, lines 45-48].

With respect to the claim, Tsuria fails to teach pairing more than one security module to a particular reception equipment and transmitting an updated list of external security module identifiers to the digital data reception equipment. Kahn teaches pairing more than CAM (security module) to an IRD (digital reception equipment) based on the generation of a selective list (0041). As an option, a selective list, converse to blacklists, can specify which CAMs an IRD can successfully pair with. As later generations, selective lists are used to identity CAMs which can be paired to an IRD while preventing others from being paired because of their security demise (0043).

Kahn shows that and IRD can contain a list of all the CAMs that it may pair with. Absent of being on the list, precludes a particular CAM from being paired. Kahn teaches that security modules that have been comprised/hacked/cloned can be removed from the selective list, effectively blacklisting them to prevent illegal content decoding. As such, it is advantageous to prevent security modules that have been compromised from successfully decoding protected content. Kahn teaches a way of doing this by using selective list identifying legitimate external security module identifiers. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results.

As per claim 30, Tsuria teaches it comprises a decoder and in that the external security module (6, 8) is an access control card (6) containing information about access rights of a subscriber to said digital data, matching being done between said decoder and said card (col. 2, lines 45-55).

As per claim 31, Tsuria teaches a decoder and in that the external security module (6, 8) is a removable security interface (8) provided with a non-volatile memory and that is designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), to manage access to said digital data, matching being done between said decoder and said removable security interface (col. 1, lines 55-60 and col. 2, lines 45-55).

As per claim 32, Tsuria teaches a decoder provided with a removable security interface (8) with a non-volatile memory and that is designed to cooperate firstly with said decoder and secondly with a plurality of conditional access control cards (6) and in that matching is done between said removable security interface (8) and said access control cards (col. 2, lines 45-55).

As per claim 36, Tsuria teaches a removable security interface including a non-volatile memory and designed to cooperate firstly with digital data reception equipment having a decoder and secondly, having and secondly with a plurality of conditional access control cards to manage access to digital data distributed by an operator, each access control card having a unique identifier and containing information about access rights of a subscriber to said digital data, with said removable security interface further comprising means for recording the identifier of each access control card in said non-volatile memory (col. 1, lines 61-65 and col. 3, lines 1-5), and at least one data processing algorithm for use by said decoder to activate or deactivate the pairing of the reception equipment to the controls cards (col. 7, lines 44-53).

With respect to the claim, Tsuria fails to teach pairing more than one security module to a particular reception equipment. Kahn teaches pairing more than CAM (security module) to an IRD (digital reception equipment) based on the generation of a selective list (0041). As an option, a selective list, converse to blacklists, can specify

which CAMs an IRD can successfully pair with. As later generations, selective lists are used to identity CAMs which can be paired to an IRD while preventing others from being paired because of their security demise (0043). Kahn shows that and IRD can contain a list of all the CAMs that it may pair with. The absence of being on the list precludes a particular CAM from being paired. Kahn teaches that security modules that have been comprised/hacked/cloned can be removed from the selective list, effectively blacklisting them to prevent illegal content decoding. As an example, an IRD came be prevented from using an older CAM but then allowed to successfully pair with a newer generation CAM for security reasons. As such, it is advantageous to prevent security modules that have been compromised from successfully decoding protected content. Kahn teaches a way of doing this by using selective list identifying legitimate external security module identifiers. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results.

As per claim 37, Tsuria teaches a PCMCIA card on which digital data descrambling software is installed (col. 1, lines 10-15).

As per claim 38, Tsuria teaches the removable security interface consists of a software module (col. 6, lines 50-54).

As per claim 39, Tsuria teaches an executable computer program stored in a computer readable medium of a digital data reception equipment (2) that can cooperate

with a plurality of external security modules (6, 8) each having a unique identifier and in which information about access rights of a subscriber to digital data distributed by an operator are stored, said digital data reception equipment comprising a computer for executing said executable computer program includes instructions for:

verifying whether or not the identifier in said external security modules (6, 8) is already memorized in the digital data reception equipment (2) upon connection of said external security modules (6, 8) to the digital data reception equipment [second card is inserted in to the receiver to validate and identify the signature of said second card; col. 7, lines 44-53] ,

activating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier of the external security modules (6, 8) is already memorized in the digital data reception equipment (2) [chaining data; col. 7, lines 45-48] and

deactivating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier in the external security modules (6, 8) is not already memorized in the digital data reception equipment (2) [inherent that if the smart card's signature is not validated, there will be no pairing; col. 7, lines 45-48].

With respect to the claim, Tsuria fails to teach pairing more than one security module to a particular reception equipment and transmitting an updated list of external security module identifiers to the digital data reception equipment. Kahn teaches pairing more than CAM (security module) to an IRD (digital reception equipment) based

on the generation of a selective list (0041). As an option, a selective list, converse to blacklists, can specify which CAMs an IRD can successfully pair with. As later generations, selective lists are used to identity CAMs which can be paired to an IRD while preventing others from being paired because of their security demise (0043). Kahn shows that and IRD can contain a list of all the CAMs that it may pair with. Absent of being on the list, precludes a particular CAM from being paired. Kahn teaches that security modules that have been comprised/hacked/cloned can be removed from the selective list, effectively blacklisting them to prevent illegal content decoding. As such, it is advantageous to prevent security modules that have been compromised from successfully decoding protected content. Kahn teaches a way of doing this by using selective list identifying legitimate external security module identifiers. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results.

As per claim 40, Tsuria teaches instructions to locally generate matching control parameters of the reception equipment (2) with an external security module (6, 8) as a function of a signal transmitted to said reception equipment (2) by the operator (col. 6, lines 55-60).

As per claim 41, Tsuria teaches instructions intended to check if the identifier of said external security module (6, 8) is memorized in the reception equipment (2), at

each later use of an external security module (6, 8) with the reception equipment (col. 3, lines 15-20).

As per claim 43, Tsuria teaches said signal is transmitted to a reception equipment (2) in an EMM message specific to an 25 external security module (6, 8) associated with this reception equipment (col. 6, lines 55-60).

As per claim 44, Tsuria teaches a signal is transmitted to a reception equipment (2) in an EMM message specific to this reception equipment (col. 6, lines 55-60).

As per claim 45, Tsuria teaches a signal is transmitted to a group of reception equipment (2) in an EMM message specific to a group of external security modules (6, 8) associated with said reception equipment (col. 6, lines 55-60).

As per claim 46, Tsuria teaches signal is transmitted to a group of reception equipment (2) in an EMM message specific to said group of reception equipment (col. 6, lines 55-60).

As per claim 47, Tsuria teaches said check signal is transmitted in a private flow processed by a dedicated software executable in each reception equipment as a function of the identifier of the external security module associated with said reception equipment (col. 6, lines 55-60).

Claims 33-35 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria in view of USP 7,457,967 to Cocchi et al., hereinafter Cocchi.

.

As per claim 33, Tsuria teaches a decoder that can cooperate with a plurality of external security modules (6, 8) to manage access to audiovisual programs distributed by an operator, each external security module (6, 8) having a unique identifier and including at least one data processing algorithm, with said decoder in comprising means responsive to said processing algorithm for executing orders sent by the operator for:

verifying whether or not the identifier in said external security modules (6, 8) is already memorized in the digital data reception equipment (2) upon connection of said external security modules (6, 8) to the digital data reception equipment [second card is inserted in to the receiver to validate and identify the signature of said second card; col. 7, lines 44-53] ,

activating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier of the external security modules (6, 8) is already memorized in the digital data reception equipment (2) [chaining data; col. 7, lines 45-48] and

deactivating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier in the external security modules (6, 8) is not already memorized in the digital data reception equipment (2) [inherent that if the smart card's signature is not validated, there will be no pairing; col. 7, lines 45-48].

For the record, “a decoder that can” implies intended use, not functional descriptive material.

With respect to the claim, Tsuria fails to teach transmitting an updated list of external security module identifiers to the digital data reception equipment. Cocchi teaches transmitting an updated list of external security module identifiers to the digital data reception equipment (col. 11, lines 37-57). Tsuria teaches that once a time expiration has occurred the smart cards will not decode the content. Cocchi teaches another reason why decoding may be prevented. Cocchi teaches that security modules that have been comprised/hacked/cloned can be blacklisted to prevent them from decoding protected content (col. 11, lines 28-35). As such it is advantageous to prevent security modules that have been compromised from successfully decoding protected content. Cocchi teaches a way of doing this by sending updated list external security

module identifiers. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results.

As per claim 34, Tsuria teaches external security modules (6, 8) are access control cards (6) in which information about access rights of a subscriber to digital data distributed by an operator are stored (col. 2, line 38).

As per claim 35, Tsuria teaches external security modules (6, 8) are removable security interfaces (8) including a non-volatile memory that can cooperate firstly with the decoder and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator (col. 6, lines 52-60).

As per claim 42, Tsuria teaches a system comprising a management platform and a digital data reception equipment (2) connected to services broadcasting network, for communication with the digital data reception equipment and with the digital data reception equipment (2) being paired with a plurality of external security modules (col. 1, lines 61-65 and col. 3, lines 1-5), each having a unique identifier wherein the system further comprises:

a first module arranged in said commercial management platform (1) for generating matching queries (col. 3, lines 15-20),

a second module arranged in said digital data reception equipment (2)

that will process the generated queries from the first module to prepare a pairing configuration to control said pairing (col. 3, lines 20-35), using pairing control parameters generated by a computer in said digital data reception equipment based upon [chaining data]

verifying whether or not the identifier in said external security modules (6, 8) is already memorized in the digital data reception equipment (2) upon connection of said external security modules (6, 8) to the digital data reception equipment [second card is inserted in to the receiver to validate and identify the signature of said second card; col. 7, lines 44-53] ,

activating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier of the external security modules (6, 8) is already memorized in the digital data reception equipment (2) [chaining data; col. 7, lines 45-48] and

deactivating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier in the external security modules (6, 8) is not already memorized in the digital data reception equipment (2) [inherent that if the smart card's signature is not validated, there will be no pairing; col. 7, lines 45-48].

With respect to the claim, Tsuria fails to teach transmitting an updated list of external security module identifiers to the digital data reception equipment. Cocchi teaches transmitting an updated list of external security module identifiers to the digital data reception equipment (col. 11, lines 37-57). Tsuria teaches that once a time

expiration has occurred the smart cards will not decode the content. Cocchi teaches another reason why decoding may be prevented. Cocchi teaches that security modules that have been comprised/hacked/cloned can be blacklisted to prevent them from decoding protected content (col. 11, lines 28-35). As such it is advantageous to prevent security modules that have been compromised from successfully decoding protected content. Cocchi teaches a way of doing this by sending updated list external security module identifiers. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/NATHAN FLYNN/
Supervisory Patent Examiner, Art Unit 2431